Lampi di Cassandra/ Lo SPID è nato morto?

(369)—I sistemi di autenticazione a due fattori gestiti tramite SMS soffrono di problemi strutturali, suggerisce una ricerca…

Lampi di Cassandra/ Lo SPID è nato morto?

Figure 1:

(369)—I sistemi di autenticazione a due fattori gestiti tramite SMS soffrono di problemi strutturali, suggerisce una ricerca dell'Università di Amsterdam. SPID-2 si basa proprio su questo meccanismo.

Probabilmente persino alcuni dei 24 informatissimi lettori non conoscono SPID, acronimo di "Sistema Pubblico di Identità Digitale", che si autodefinisce "La soluzione per accedere a tutti i servizi online della pubblica amministrazione e dei privati con un'unica Identità Digitale". Perciò, prima di passare a fosche profezie, Cassandra è obbligata a fornire qualche informazione, peraltro facilissimamente reperibile in Rete. Dunque, SPID, noto anche a chi ha memoria lunga come "Il PIN di Renzi", è un sistema pubblico di creazione e distribuzione di identità digitali, controllato dallo Stato Italiano e realizzato da fornitori privati da esso certificati ed iscritti un un apposito Albo.Viene infatti gestito esattamente come è stato fatto per la Posta Elettronica Certificata con la quale, per fortuna, si sono creati sia un utile strumento per il cittadino che un onesto business per alcune aziende di servizi informatici.I problemi che attualmente affliggono lo SPID sono di due tipi: commerciali e tecnici.

Quello commerciale, dovuto al solito bando confezionato ad arte ("solo aziende con almeno 5 milioni di euro di fatturato") pare sia stato risolto di recente.

I problemi tecnici sono appena cominciati, ma preoccupano già molto: vediamo un attimo perché.Chi ha bisogno di una identità digitale la compra da un fornitore a scelta: attualmente

ce ne sono tre.

I fornitori, dotati di adeguata struttura amministrativa e tecnica certificata, effettuano il riconoscimento della persona, ne verificano l'identità e rilasciano le credenziali richieste. Con queste credenziali l'utente si potrà (prossimamente) autenticare a tutti i siti e servizi delle pubbliche amministrazioni, ed a tutti i siti e servizi commerciali che la vorranno adottare.

E per i primi due anni le credenziali sono anche gratuite."Tutti" e "Gratis". Bello eh?

Si, ma anche no, e vediamo perché.

Esistono tre tipi di credenziali: SPID-1, SPID-2 e SPID-3.SPID-1 è un nome utente fisso con una password modificabile dall'utente: buono per autenticarsi su un social o una mail list, ma certo non buono per una dichiarazione dei redditi, un pagamento, un voto o la presentazione di un bilancio. Secondo Cassandra non avrebbe nemmeno dovuto esistere perché implementa una cultura dell'insicurezza.SPID-3: autenticazione con token digitale. Per ora nessuno la fornisce, quindi è difficile darne un giudizio, se non che è la triplicazione di altri due servizi che potrebbero essere usati con la stessa efficacia, cioè dispositivo di firma digitale e carta nazionale dei servizi (di solito coincide con la tessera sanitaria). Essendo non una duplicazione ma una triplicazione anche SPID-3 non dovrebbe esistere.SPID-2 è una autenticazione a due fattori, nome utente e password, congiuntamente alle generazione di un codice temporaneo che viene inviato via SMS o con app mobile dedicata. Già diffuso ed usato soprattutto dalle banche, è realizzabile anche in una diversa, più sicura e più costosa versione, in cui il codice temporaneo viene generato ogni minuto da un piccolo token con display LCD che si tiene in casa o nel portachiavi.SPID-2 non prevede tuttavia l'uso di un token fisico, ma solo della versione SMS. E qui vengono i dolori.

infatti stata pubblicata un'interessantissima ricerca dell'Università di Amsterdam dal titolo "How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication", cioè "Come l'integrazione di smartphone e pc ha appena ucciso l'autenticazione a due fattori via SMS". Si parla appunto delle ben note sincronizzazioni nei vari cloud e tra i vari sistemi operativi dei nostri gadget tecnologici, tanto comode ma anche tanto rischiose, e non solo per la privacy.

Le 17 lucide pagine descrivono dettagliatamente l'implementazione di attacchi mirati per violare i sistemi con codice temporaneo via SMS, sia in ambiente Android che iOS, con una prosa precisa ed implacabile, concludendo che mantenere ragionevolmente sicura l'autenticazione a due fattori via SMS sarà una sfida difficile e costosa. Per chi non troverà il tempo di leggere il paper (e farà male) è importante sottolineare che il problema segnalato non riguarda il semplice exploit di un paio di bachi, che poi saranno corretti in modo da risolvere il problema stesso. Il problema delineato è più sistemico e più profondo, quindi anche più grave e difficilmente correggibile, visto che contrasta con l'usabilità di prodotti. il problema di permettere a più device di sincronizzarsi automaticamente ed in vario modo tra di loro e col cloud. Meccanismi di questo tipo, che si moltiplicano continuamente perché sempre più necessari, sono violabili anche senza veri e propri bachi software, perché dovendo far parlare device diversi tra loro senza disturbare troppo l'utente (e quindi avere prodotti più "belli") saranno sempre intrinsecamente deboli perché, per spinte commerciali, devono essere prima di tutto flessibili e facili da usare.Così la sicurezza, da sempre Cenerentola dell'elettronica di consumo, sarà considerata ancora meno, quando invece il paper, nelle sue conclusioni, sottolinea che i problemi intrinseci di sicurezza diverranno sempre più gravi fino al limite dell'ingestibilità. Leggetevelo, anche perché all'Agenzia per l'Italia Digitale non hanno probabilmente avuto il tempo per farlo.

Se SPID-2 fosse invece un'autenticazione a due fattori con token hardware, anche se suscettibile di attacchi tipo Man-in-the-Browser (MitB), sarebbe comunque di gran lunga più difficile da violare e soprattutto da violare su larga scala.

E quindi? Quindi anche se SPID-2 non è nato proprio morto, è purtroppo un neonato a gravissimo rischio. Cassandra la ritiene una soluzione decisamente sconsigliabile, come le sue due sorelle.Nulla rimane da dire quindi sullo SPID come iniziativa digitale italiana.Il problema più vasto di avere una identità digitale univoca merita invece qualche altra considerazione.La violazione delle vostre (ipotetiche) credenziali SPID implica pericoli molto più gravi del semplice svuotamento del vostro conto corrente. Le credenziali sono "voi", dovunque. Devono essere sicure ed utilizzate con attenzione.Essendo uniche potrebbero essere usate per impersonarvi e realizzare azioni su innumerevoli siti e servizi di cui voi nemmeno conoscete l'esistenza.

Ecco perché, secondo Cassandra, per SPID vale quanto detto a suo tempo per la CEC-PAC ed altre storie dell'orrore digitale italiane.

Neanche gratis.

Originally published at punto-informatico.it.

By Marco A. L. Calamari on February 8, 2022.

Canonical link

Exported from Medium on August 27, 2025.